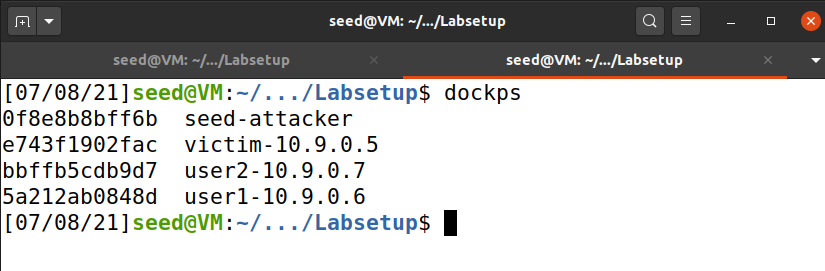
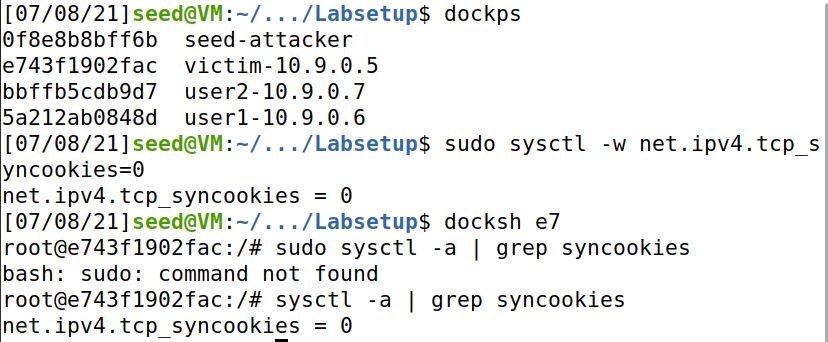
**TCP/IP Attack Lab**

**Task 1: SYN Flooding Attack**

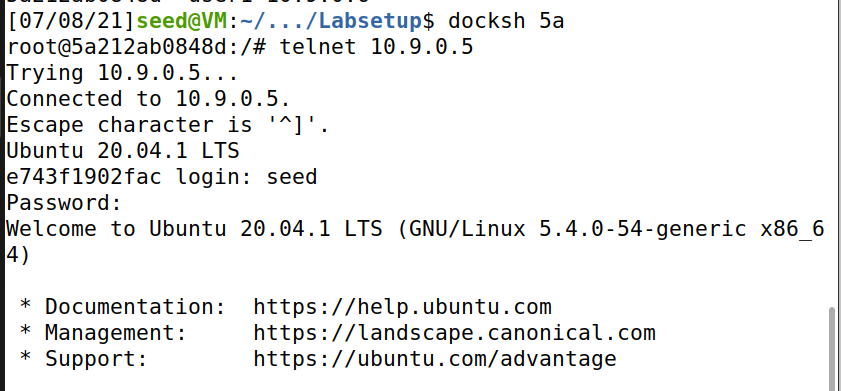
攻击者为10.9.0.1，受害主机为10.9.0.5，两个观察者为10.9.0.6和10.9.0.7



在受害主机10.9.0.5上关闭SYN Cookie，需要注意的是，容器没有修改SYN的权限，因此我们必须在创建容器时关闭SYN Cookies

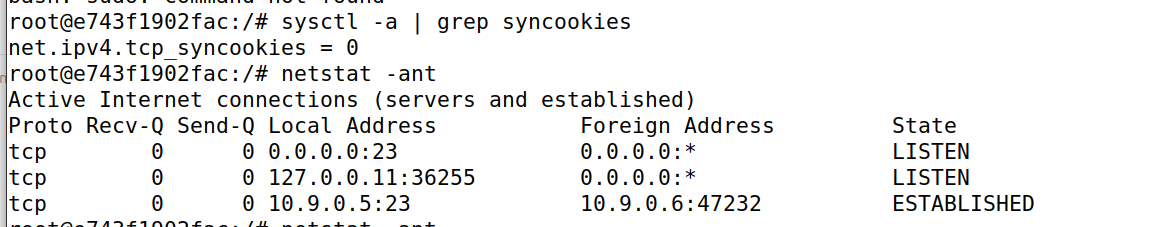


开始前，使用user1尝试登陆受害主机10.9.0.5，发现可以成功登录

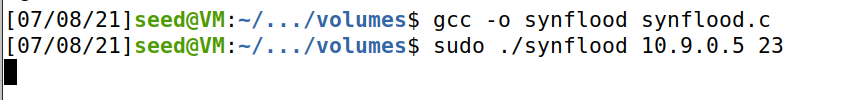


在开始攻击之前，检查一下受害主机10.9.0.5上的半开放连接数

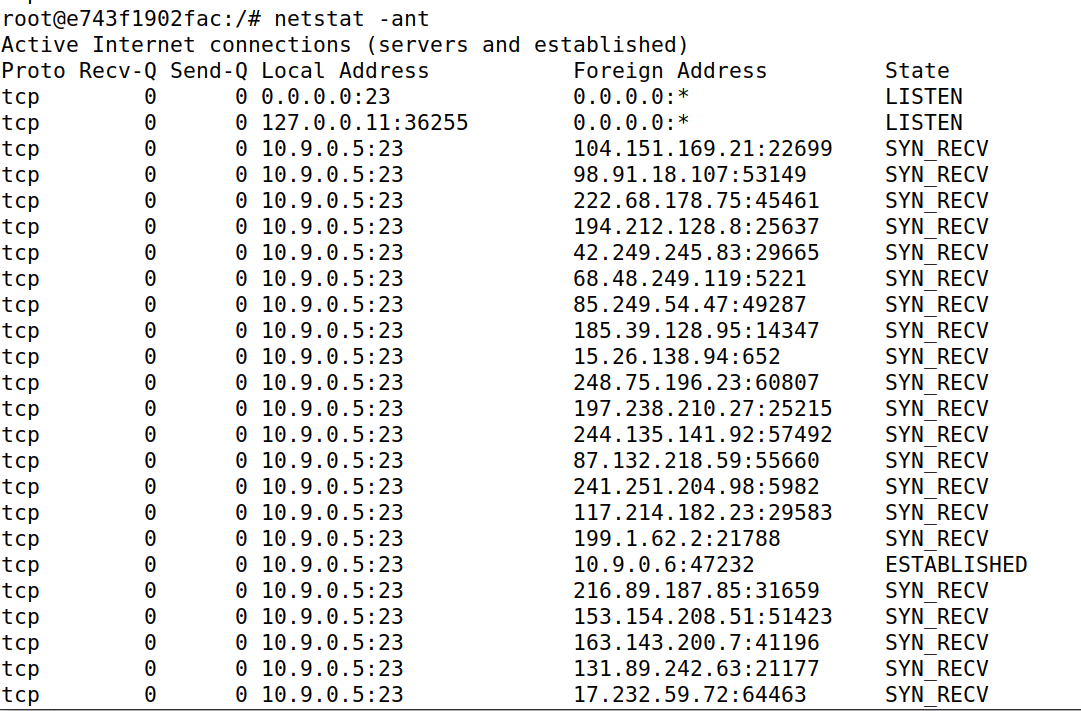
由下图可以知道，均为LISTEN状态，并没有发现SYN\_RECV状态的半连接



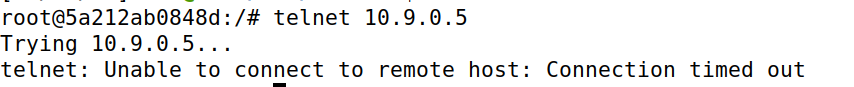
在攻击主机中运行脚本，进行泛洪攻击



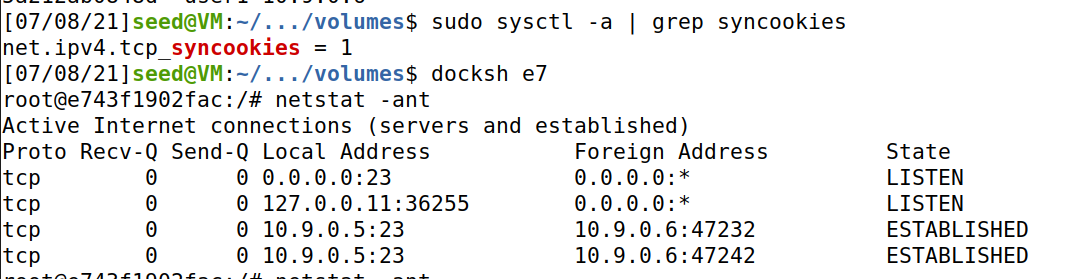
再次使用netstat -ant命令查看受害机，发现有很多SYN\_RECV状态的链接，说明已经遭受了SYN泛洪攻击



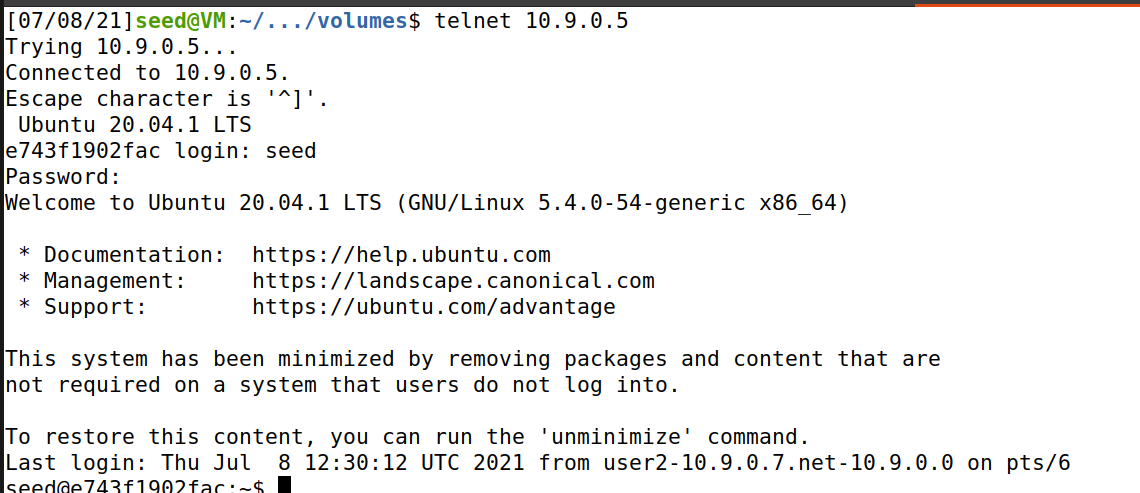
使用user1 10.9.0.6尝试登录受害主机10.9.0.5，发现无法登录



重新打开SYN Cookie

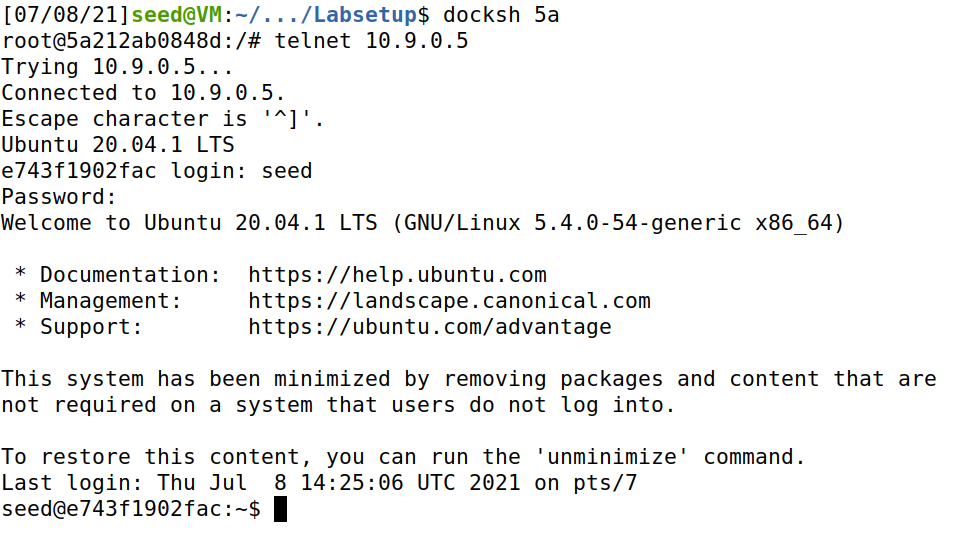


发现在SYN泛洪攻击下，仍可以访问被害主机10.9.0.5

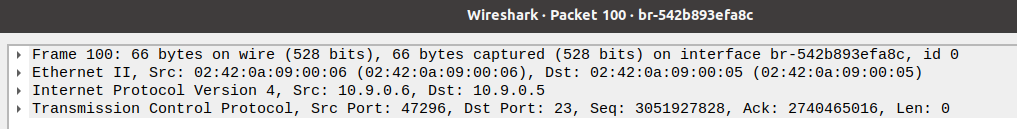


**Task 2：TCP RST Attacks on telnet Connections**

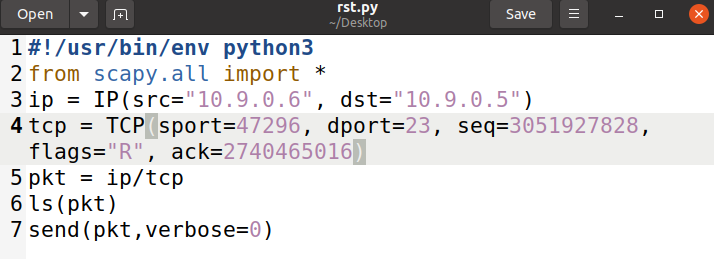
进行RST攻击破坏telnet之间的连接



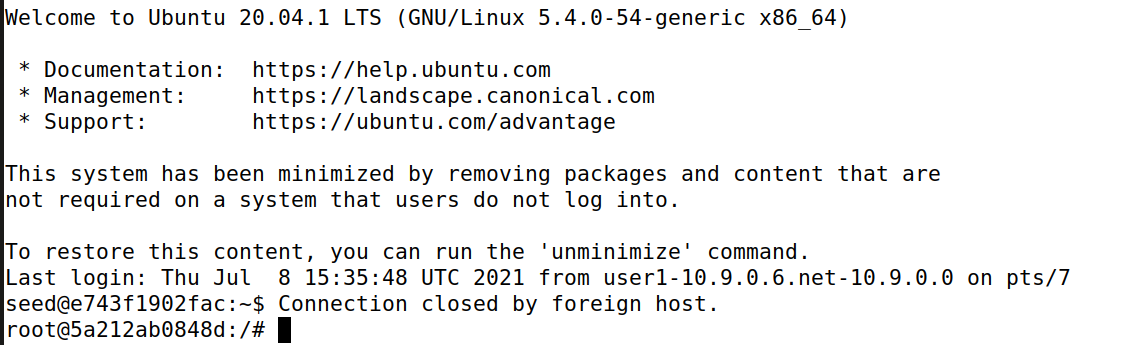
使用wireshark抓包，获取tcp报文



编写脚本，对tcp包进行修改，发送RST包

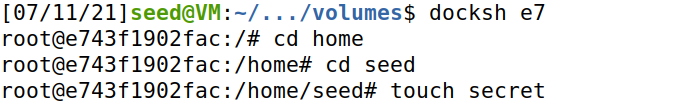


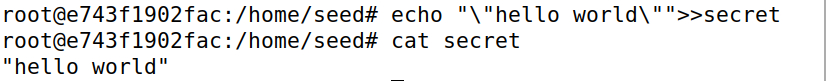
执行脚本，发现telnet连接中断



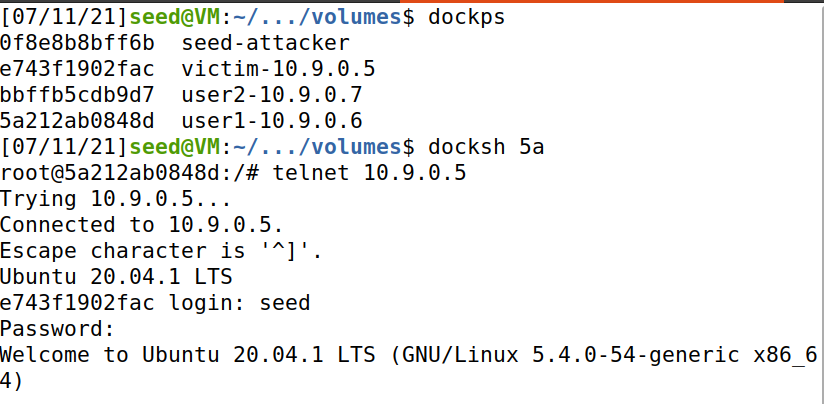
**Task 3: TCP Session Hijacking**

为了验证攻击是否成功，我们事先进入受害主机，在seed目录下创建一个文档secret,攻击的目的就是为了输出secret里面的内容

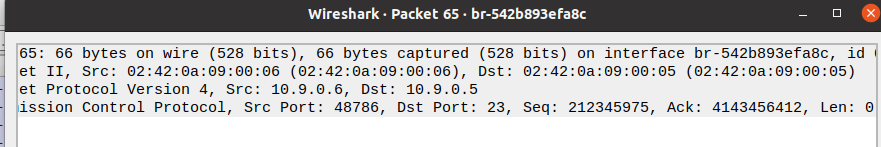




登录容器，使用user1 10.9.0.6尝试远程登录受害者主机10.9.0.5，建立telnet连接



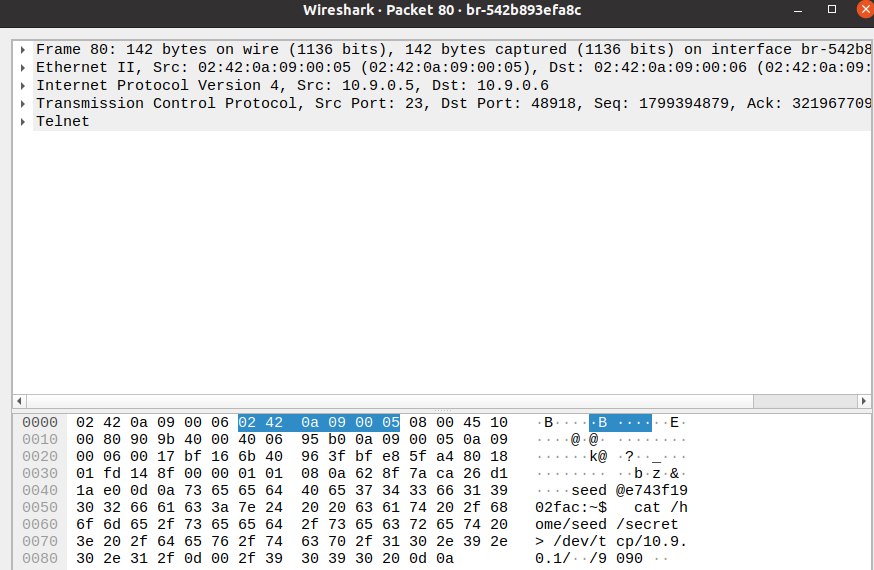
使用wireshark进行抓包，找到最后一个包，获取端口信息



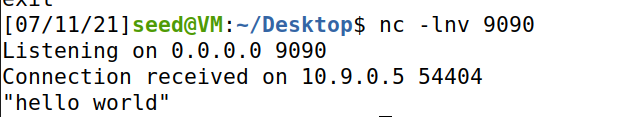
编写脚本，并且运行，以此进行TCP会话攻击



再次使用wireshark进行抓包，查看可以看到我们伪造的数据成功发送

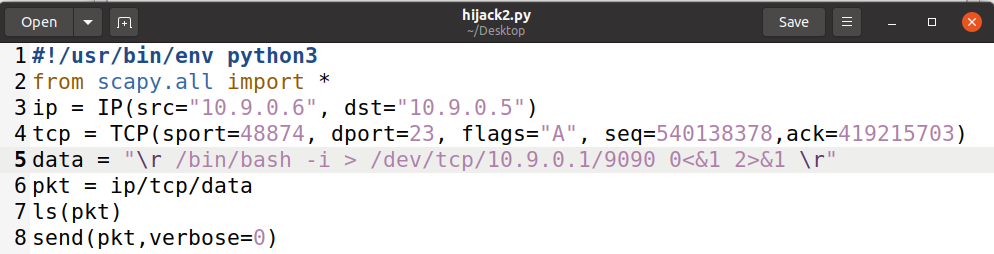


在seed主机查看运行结果，发现受害机成功运行了我们的命令，将secret里面的内容发送给了攻击者10.9.0.1、9090，说明劫持成功

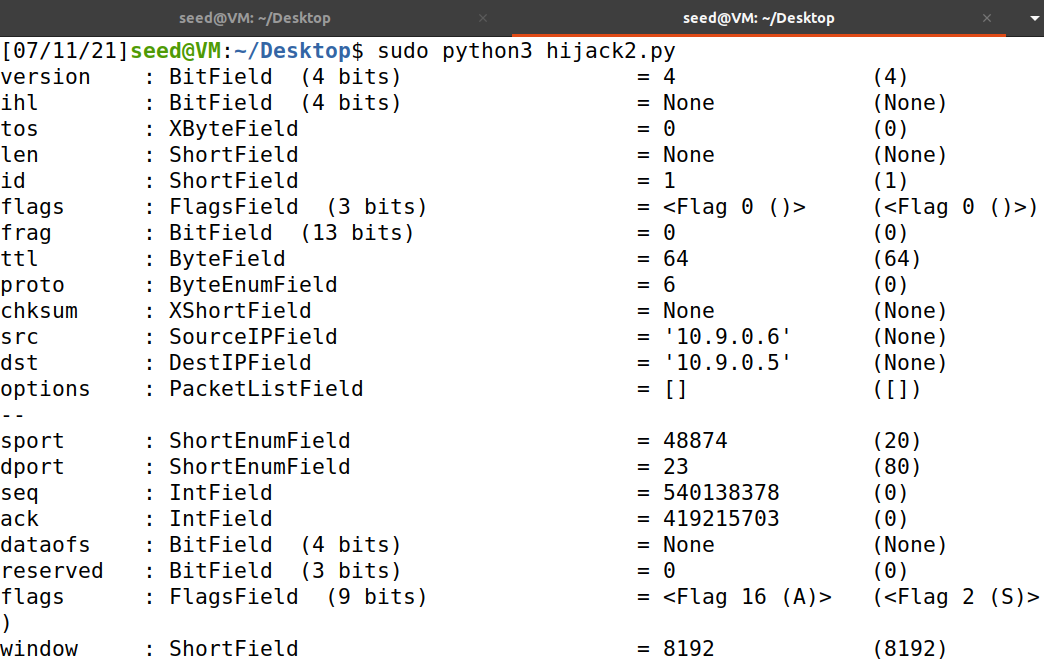


**Task 4: Creating Reverse Shell using TCP Session Hijacking**

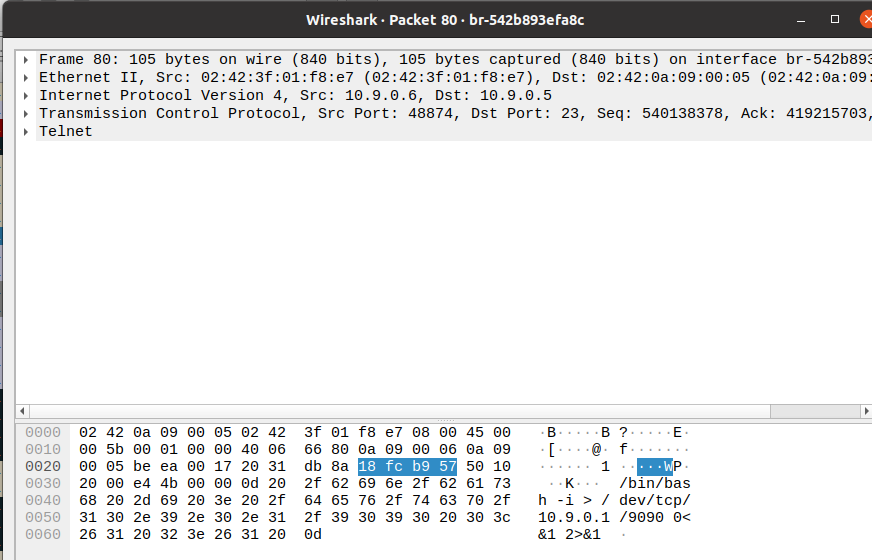
抓包，并根据里面的信息编写脚本，内容如下，需要发送命令到受害主机



运行脚本



查看发送的数据包



最后我们成功的建立了shell连接，说明攻击成功

